

Social networking



Social networking websites allow you to communicate and share information. But they can also be used to spread malware and to steal personal information.

Social networking sites, such as Facebook and Twitter, continue to grow in popularity as attack vectors. Unscrupulous individuals can use information you post online to learn details about you that can be useful for social engineering or guessing the answers to security questions on other websites. Attackers may also compromise an account of a friend and use it to distribute malware or other malicious content.



Be cautious about what links you click on. Make sure any computer you use to connect to the site is protected with the latest security software and patches. Use strong passwords and use separate passwords for each account. Take advantage of two factor authentication, if available. Be thoughtful about what you post online, and use available privacy settings to limit who can see your information.



How to be safe on the Internet.

- ✓ Keep up-to-date with security patches
- ✓ Use firewalls
- ✓ Don't follow links in unexpected emails
- ✓ Use different passwords for every site



**BEWARE OF
UNEXPECTED OR
UNKNOWN EMAIL AND
ATTACHMENT**



www.google.com

moviewriternyu wordpress.com